TITLE OF THE INVENTION

Method to enable Heartbeat e9-1-1

CROSS-REFERENCE TO RELATED APPLICATIONS

Utility Patent Filing, application number 10/605144, EFS ID 47552, date time group 2003-09-11 10:55:59 EDT titled "method to commercialize structured military messaging" by inventor Steven J. McGee. Utility Patent Filing, application number 10/708000, EFS ID 54568, date time group 2004-01-30 20:06:41 EDT titled "Method to enable a Homeland Security Heartbeat".

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

The Department of Homeland Security forwarded this method to enable Heartbeat e9-1-1 to the federal government's Technical Support Working Group – TSWG who tabled this inventor's proposed invention on 11 January 2006. The TSWG is comprised of board members from the major anti-terrorism agencies (e.g., FBI, CIA, NSA, DHS, DIA and DOD).

NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT

Not Applicable

INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISK

Not Applicable

BACKGROUND OF THE INVENTION

Field of the Invention

This invention is a second continuation of two previous method patent applications relating to homeland defense and homeland security network centric warfare in the area of situational awareness, alerting, emergency response telecommunications and inter complex system networking enabling "spontaneous integration" or (re) task organization by disparate, adhoc military / commercial sector units.

The unique nature of this invention rests on the fact that the military system of systems and commercial systems apply the heartbeat protocol and heartbeat XML network (re) configuration messages as common building blocks and methodology – differently. Currently, network centric warfare procedures and methodology are applied to the military's organic communications but not the communications that it leases that often comprise up to 80% of the total telecommunications portfolio.

The military's core situational awareness systems and our emergency systems rely on the heartbeat protocol and heartbeat XML messages albeit with different (military unique / XML message hybrid) schema structures, event refresh timing, and symbol sets. This application method to enable Heartbeat e9-1-1 together with its two preceding method patent applications describes a methodology to achieve interoperability and operational synergy between military "system of system" equipped units and disparate commercially supported units improving interoperability while increasing the military's network centric warfare efficiency.

One of the DHS's top three long term goals is (enabling) "A national common operating picture for critical infrastructure". A congressional directive states "nothing less than network centric homeland security akin to network centric warfare". A Department of Homeland Security document describing state interoperability funding dated May 2006 states on page 32: a goal to "Improve capacity to include Emergency Medical Service responder status management and vehicle location as an extension of the HEARTBEAT computer aided dispatch system".

The military provides 20% of its network capacity in South West Asia. The remaining 80% is leased commercial (portfolio) assets. Applying network centric warfare procedures to 100% of their portfolio is not only Clinger-Cohen Act compliant (see response to the USPTO non final rejection mailing for application number 10/605144). The unique nature of the second filing (10/708000) is describing a common, consistent, standard method of applying the heartbeat protocol and heartbeat messages across x complex systems, y federal, state and local contracts, and z product and system types in a universal, non-proprietary military unique method.

Method to enable Heartbeat e9-1-1 focuses interoperability efforts on the heartbeat protocol and heartbeat XML message / schema network centric warfare common denominators / building blocks commercializing military methodology to apply through the world's telecommunications emergency / disaster alerting infrastructure (e.g., Public Safety Access Points or PSAPs) via child schemas and or military data elements (situation dependent) residing in data islands embedded in parent Common Alert Protocol – CAP schemas.

This invention describes a method whereby network centric warfare (NCW) procedural methods currently applied to military networks in a proprietary method (e.g., Tactical Data Links or TADIL formats are military developed, unique binary formats as described in method patent application 10/605144 "method to commercialize structured military messaging") are commercialized then reapplied to commercial emergency networks (e.g., E9-1-1 Public Safety Answering Points – PSAPs).

The base application 10/605144 describes a methodology where military unique FFIRN (field item reference numbers and FUDNS (field unit number designators) that are three and four digit codes are converted to corresponding DOD Discovery Metadata Standard – DDMS XML tags; these tags as part of XML forms / messages / schemas (only different in name and in structure) will be processed by Commercial Off the Shelf (COTS) products like Groove or Biztalk or any product with an intrinsic forms engine / XML parser. Symbolic interoperability and interoperable data exchange is 10/605144's intent.

The first continuation method patent application 10/708000 "method to enable a Homeland Security Heartbeat" describes methodology enabling consistency of event timing / network configuration data harvesting across n complex systems for event data distribution and network (re) configuration and reconstitution based upon the TCP/IP heartbeat protocol that is a low level publish – subscribe mechanism in widespread use by both military and commercial systems – applied differently (e.g., the heartbeat data collection is set at different temporal rates).

Application 10/708000 adds through the use of the heartbeat protocol's intrinsic timing function and data harvesting function adds temporal consistency and the ability to "spontaneously re-integrate" based on the military's system development enabling organizational mobility via multicast / unicast router/switch groups managed by Management Information Bases – MIBS.

Application 10/708000 describes a methodology whereas router-switch multicast groups for tactical-strategic military systems, first responder and commercial event-alert broadcast services are updated at heartbeat protocol set predefined intervals (e.g., milliseconds, seconds, & minutes). This multicast descriptive group data stored in Management Information Bases (MIBS) in router/switches is updated by data gathered by the heartbeat protocol as a type of publish subscribe mechanism. This network configuration data is then distributed by eXtensible Markup Language - XML heartbeat schemas / messages / forms (functionally the same) that are used to reconfigure unicast – multicast network parameters such as router – switch management information bases (MIBs).

According to the AFCEA Signal Magazine reference below, one of the key systems formats is part military unique (Variable Message Format) and part XML schema that will not be directly exchanged (e.g., messaging) with our commercial emergency notification network (e.g., PSAPs). DOD's application of the heartbeat protocol & heartbeat messages:

2

Armed Forces Communication's Electronics Association' AFCEA's SIGNAL Magazine article "Defense Knowledge Management Hinges on Compatibility" May 2005. "Using Web services technology and a laptop computer, these researchers separated the Force XXI Battle Command Brigade and Below - FBCB2 application from Blue Force Tracking data according to an established schema. An extensible markup language (XML) wrapper exposed the discovery metadata to a portal for updating every thirty seconds".

Thirty second web server refresh rates are insufficient for engagement of objects traveling towards targets at speeds approaching or exceeding mach -- hence the need for direct data / message (binary) XML schema exchanges between military and first responder situational awareness systems (e.g., Heartbeat e9-1-1). The most pressing case is the need to exchange data between Federal Aviation Administration PSAP supported networks processing NORAD telemetry data directly with military units of action (i.e., military jets) – other wise described as the September 11th scenario.

The inventor will now list precedent commercial initiatives on which to achieve operational synergy with military derived situational awareness methodology.

AT&T has developed a movement detection process that it calls the "Heartbeat Solution." AT&T has designed its Voice over Internet Protocol - VoIP telephone adapters to enable it to detect when an adapter has been disconnected and then reconnected. Once the Heartbeat Solution detects a reconnection, "the AT&T network will temporarily suspend the customer's service and will post a message at the customer's web portal directing the customer to confirm the existing registered location address or register a new location address."

The Emergency Management Network (EMnet) in use in a dozen states "generates Nadat HEARTBEAT messages to maintain lost connection. EMnet/Emergency Action System (EAS) messages will be delivered to broadcasters within seconds using the secure satellite delivery system".

During the 2006 National Football League Super Bowl, an approach to fuse sensor data was demonstrated by the 51st Michigan National Guard involving the Transducer Data Exchange Protocol (TDXP). TDXP is implemented over IETF 1451 that interact with Management Information Bases (MIBS) that rely on the heartbeat protocol.

Raytheon / XM Satellite Radio's approach is described "NYC Firefighters plan a military approach to command and control". By viewing information displayed as an electronic map, fire department commanders will be able to move firefighters, equipment and emergency medical teams around in much the same way military commanders shift troops and equipment around a battlefield".

Cisco Systems Communications Interoperability and Safety Systems - IPICS is "based on proven IP standards"" the Cisco IPICS server is monitored using a "heartbeat". "IPICS software uses XML messaging schemas to identify types of communications devices managed by the system."

Eaton Inc's "Home Heartbeat" as the "World's First Home Awareness System" as an example of the technology backed by the ZigBee Alliance of 100 companies employing the ZigBee mesh networking protocol that makes use of the underlying heartbeat protocol. The inventor believes that this community is building a logical bridge to exchange situational awareness data in our neighborhoods with the military terrorist information producing systems that also make use of the heartbeat protocol. In addition to receiving alerts that a situation like washers overflowing or the garage door is left open when the occupants are scheduled away (an open invitation to terrorist activity), the owners and appropriate first responders will be alerted and situational awareness maps updated. Neighborhoods will be alerted in mass is say an airplane like the one that was downed in rural Pennsylvania is headed for a more populated area.

Lockheed Martin / Qualcomm & SPRINT-Nextel's Department of Justice Integrated Wireless Network (IWN) bid necessarily involves Qualcomm's role in the development of Blue Force Tracking (BFT) in the Balkans. Reason being, changing their approach would be expensive and would impact interoperability

with key military situational awareness systems e.g., FBCB2, Blue Force Tracking, Joint Blue Force Situational Awareness & Land Warrior that are still being fielded and will be in the inventory until well into the next decade.

Geospatial/Dispatch systems like Intergraph's Computer-Aided Dispatch System (I/CAD) make use of Telco location data: Automatic address input via ANI/ALI (automated number/location information) & Automatic location verification. Vehicle positions from an AVL system auto displayed on I/CAD map on 18 military installations.

Telco e9-1-1 PSAP's processing NORAD aircraft tracks and DOD SA systems processing aircraft tracks do not directly exchange messages / XML schema's with each other Given that up to 80% of a unit's communications will be commercially leased, this implies that only 20% of a force's network centric warfare supporting assets (router/switches) are employing network centric warfare practices and that if these military assets were not available, soldiers would not be able to fight as they have trained nor would they be able to discuss an event with First Responder counterparts given different temporal data collection, screen refresh rates, and geospatial symbol sets.

The heartbeat protocol and heartbeat network reconfiguration messages are part of Defense Information System Agencies (DISA) Network Centric Enterprise Services (NCES) Technology Development Strategy Version Two dated 26 May 2004. The heartbeat protocol as part of DISA's Network Centric Enterprise Services Technical Plan, Telco regulations, and bell-weather IT firms public safety strategies, is a simple but effective means to improve interoperability leveraging the power of network centric warfare.

Point being of the above listed precedents is that more modern protocols are being devised as well as current products / complex systems yet they still rely on the heartbeat protocol / heartbeat messages. Distributed Instruments states that "TDXP was designed and built for a Service Oriented Architecture SOA" supporting direct interoperability between layer one and two (mobile, chaotic environments) with enterprise level SOA(s) that implement system wide heartbeat protocol and heartbeat mechanisms to monitor supported application and system health. .

While the heartbeat protocol mechanism is not necessarily needed to time data exchanges (given the network timing protocol (NTP), the heartbeat protocol is currently and will continue to be a multi industry standard among situational awareness (SA) alerting and failover systems until well into the next decade – especially on the military side of the equation where scheduled replacement systems such as Future Combat Systems (FCS) will not be fully fielded until 2014 referencing the current military schedule. Once fielded, systems typically remain in the portfolio for a decade or more. Point being is that the heartbeat protocol and XML heartbeat message / schema's / forms will be viable for the next decade or longer.

Summarizing this section, this second continuation application 10/709358 is a continuation of 10/70800 that is a continuation of 10/605144. It describes a methodology to reapply network centric warfare procedures removing the military proprietary structured military message formats described in 10/605144 via standard XML schema structures (CAP child schemas and / or data islands in DDMS format) with commercial leased systems. This methodology improves interoperability in terms of symbology, EAC and smartphone screen refresh rates and timeliness of alerts. This invention describes a methodology whereby individuals or groups data subscriptions are updated via a common refresh rate for display on Emergency Action Center (EAC) screens and personal handheld wired and wireless mesh network supported devices (e.g., smart phones, personal digital assistants) applying a common symbology set as described by accessing common federal XML repositories described by common syntax e.g., Service Provisioning Markup Language (SPML) and Web Services Resource Framework (WSRF) that maintains state information essential in low bandwidth, mobile environments.. Disparate systems access this configuration and user subscription data from supporting (DISA) Service Oriented Architectures (SOA) that implement system wide heartbeat services via heartbeat XML messages.

Description of Related Art

BRIEF SUMMARY OF THE INVENTION

Principle Operation of the Invention: data elements derived from structured military messaging as processed by commercial forms engines with underlying message parsing processes provide the ability to resolve down to the individual platform level symbolically vice a geographic area of interest as in the Common Alert Protocol - CAP. TCP/IP's heartbeat mechanisms provide a common and consistent send to / get from plus timing / trigger function for data harvesting and exchanges adding DOD Data DDMS tagged data islands to the CAP and/or creating child domain specific schemas will provide the basis of a international Heartbeat 911 service available on a subscription basis such as neighborhood watch programs equipped with GPS smart phones, handhelds, laptops and like devices. Use of the TCP/IP heartbeat protocol and heartbeat XML messages as common denominators / common building blocks as a means to establish a common structure to improve interoperability and consistency among and between complex systems is the intent of Heartbeat e9-1-1. Heartbeat e9-1-1 addresses the interoperability challenge where unique Federal / military situational awareness (SA) systems and Telco networks supporting First Responder e9-1-1 systems agree upon the common, consistent and interoperable settings of common denominators: the TCP/IP heartbeat protocol and heartbeat (XML) messages that convey network configuration data (e.g, router MIBs / multicast group subscriptions) -- differently. When the DOD and the world's Telco networks agree on common network (re) configuration procedures based on these common denominators (heartbeat protocol and heartbeat eXtensible Markup Language (XML) Emergency Data Exchange Language Distribution Element (EDXL-DE) formatted schemas), direct data / message exchanges and collaboration based on common timing of events and common symbology will be possible.

Performing a patent search, the closest patent application that discovered using the text string "heartbeat" + protocol + messaging is the below cited application. It cites the heartbeat protocol in context with network keepalive functions / messages that this inventor does not mention once in this application.

United States Patent Application 20020164999
Kind Code A1
Johnson, William J. November 7, 2002

System and method for proactive content delivery by situational location

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

The below graphic is labeled and divided into three distinct areas corresponding to the inventor / SAW Concepts method patent applications. This graphic is derived from the same template applied by the previous two applications. The upper left hand corner labeled 1st claim area "method to commercialize structured military messaging" that is the title of method patent application 10/605144. The lower left hand corner is labeled "2nd claim area corresponds to application number 10/708000 "method to enable a homeland security heartbeat". The claim area corresponding to this application is the area on the right hand side of the diagram below and above the dashed lines. Describing each claim area in turn:

Claim area one 10/605144: As structured military proprietary military message formats as generated by the Ground Tactical Communications Server – GTCS product are converted to commercial standard XML schema's the underlying government developed message parsers will be replaced by parsers that are intrinsic to commercial products. The inventor used Groove Networks Groove's software framework as an example. Functionality of this section is fully described by 10/708000.

As the military's FFIRN (field reference numbers) and FUDs (field unit designators) that are three and four digit codes are converted to corresponding XML tags, those tags as part of XML form / messages will be processed by products like Groove or Biztalk or any other product with an intrinsic forms engine / XML parser. Symbolic and data exchange interoperability is the theme of application 10/605144.
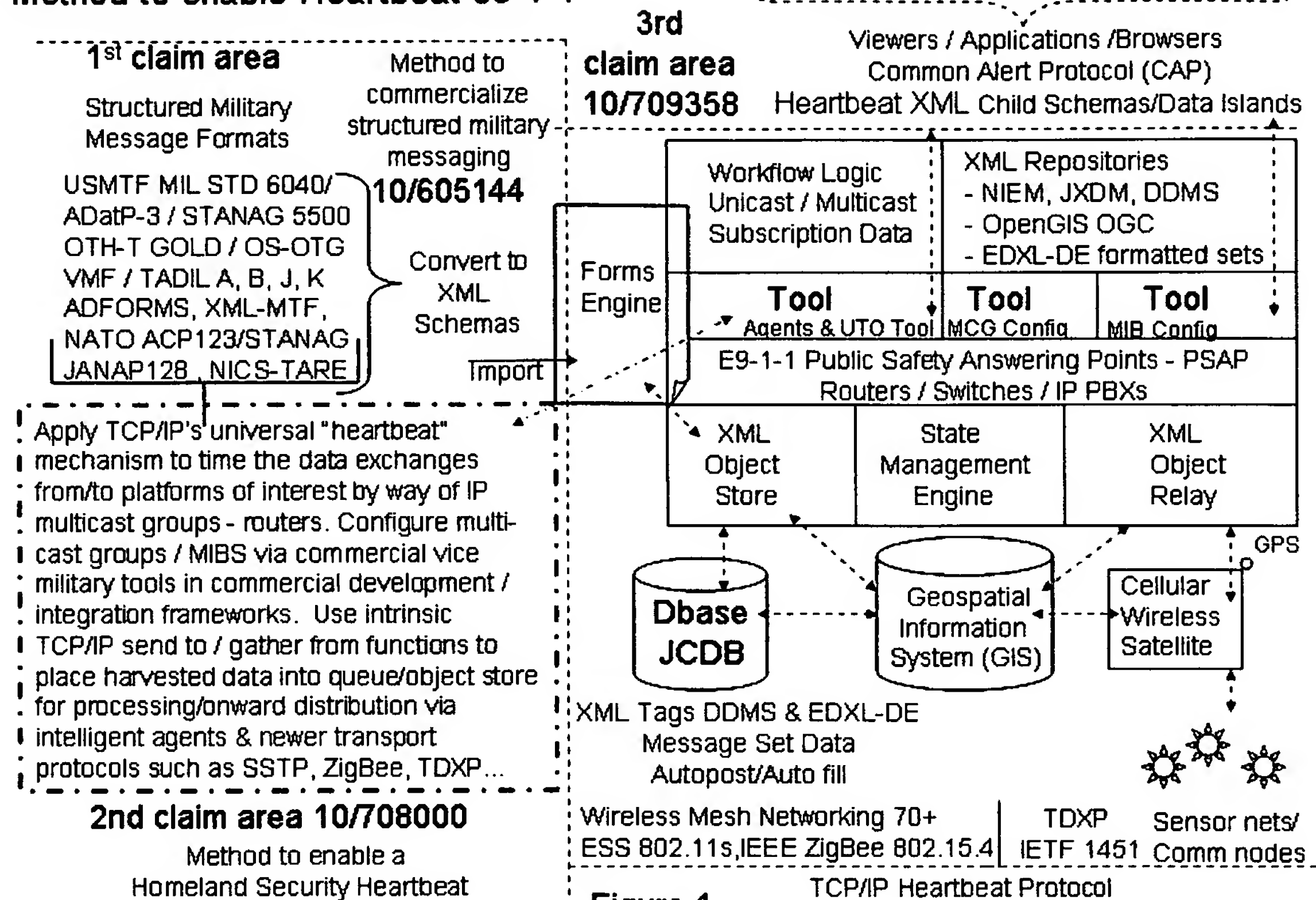
Method to enable Heartbeat e9-1-1

1st claim area

Structured Military Message Formats

USMTF MIL STD 6040/
ADatP-3 / STANAG 5500
OTH-T GOLD / OS-OTG
VMF / TADIL A, B, J, K
ADFORMS, XML-MTF,
NATO ACP123/STANAG
JANAP128, NICS-TARE

Method to commercialize structured military messaging
10/605144

Convert to XML Schemas

Import

3rd claim area 10/709358

Viewers / Applications /Browsers
Common Alert Protocol (CAP)
Heartbeat XML Child Schemas/Data Islands

Forms Engine

Workflow Logic
Unicast / Multicast
Subscription Data

XML Repositories
- NIEM, JXDM, DDMS
- OpenGIS OGC
- EDXL-DE formatted sets

Tool Agents & UTO Tool | **Tool** MCG Config | **Tool** MIB Config

E9-1-1 Public Safety Answering Points - PSAP
Routers / Switches / IP PBXs

XML Object Store | State Management Engine | XML Object Relay

Dbase JCDB

Geospatial Information System (GIS)

Cellular Wireless Satellite

GPS

XML Tags DDMS & EDXL-DE
Message Set Data
Autopost/Auto fill

Apply TCP/IP's universal "heartbeat" mechanism to time the data exchanges from/to platforms of interest by way of IP multicast groups - routers. Configure multi-cast groups / MIBS via commercial vice military tools in commercial development / integration frameworks. Use intrinsic TCP/IP send to / gather from functions to place harvested data into queue/object store for processing/onward distribution via intelligent agents & newer transport protocols such as SSTP, ZigBee, TDXP...

2nd claim area 10/708000

Method to enable a
Homeland Security Heartbeat

Wireless Mesh Networking 70+
ESS 802.11s,IEEE ZigBee 802.15.4 | TDXP IETF 1451 | Sensor nets/ Comm nodes

TCP/IP Heartbeat Protocol

Figure 1

2nd claim area 10/708000 – first continuation of 10/605144: The gathering of data / intelligence / network configuration data by the heartbeat protocol is timed consistently by the heartbeat protocol between like organizations / units. A military medical unit at the scene of a disaster or event would collaborate most efficiently if its counterpart Emergency Medical Service (EMS) team's event refresh rate were consistent to the military's (e.g., every five, fifteen minutes or faster/slower given the operational scenario / Standard Operational Procedure of the unit / organization). Too slow event refresh rates result in data that in the military system used as a template by the inventor (Force XXI Battle Command Brigade and Below – FBCB2) is described as "stale". Event refresh rates that are too frequent (e.g., milliseconds, 5 seconds...) will saturate low bandwidth links indicative of tactical / chaotic wireless network environments.

Method patent application 10/709358 – 2nd continuation of 10/708000: The heartbeat protocol as a low level data harvester gathers network configuration data (e.g., current IP lease, multicast group participation, state information such as moment greater than 50 meters, at halt, off line, or straggler...) that is gathered and forwarded by any newer, more efficient products or systems. Once multicast subscription group (s) state data is consolidated, data is consolidated by the tactical equivalent of the corporate system administrator or the S-6 in military parlance. As described in application 10/708000, the Tactical Internet Management System or TIMS is used to configure router management information bases (MIBS) and associated multicast entries describing the grouping of organizations (units) for missions (Unit Task Order). The S-6 / system administrator then broadcasts the updated network configuration data in the form of (K00.99 Variable Message Format) heartbeat messages to higher, lower and adjacent organizations refreshing router/switch unicast / multicast subscriptions. On the military side of this procedural method, situational awareness data subscriptions are updated and units tether and untether to network nodes as they maneuver. A similar process occurs on the commercial side of this methodology as cell phone / smart phone / wireless laptop users tether and untether to cell tower nodes – differently i.e., different heartbeat protocol data collection-distribution rates and different heartbeat XML message schema structures).

Method patent application 10/709358 by citing Emergency E9-1-1 cell phones and smart phones is claiming that network centric warfare methodology / procedures commercially emulated by E9-1-1 Public Safety Answering Points – PSAPs will increase the benefits of this key federal initiative while improving military to first responder interoperability and operational consistency.

DETAILED DESCRIPTION OF THE INVENTION

This application asserts that applying common operational procedures / methodology, XML message structures, and timing / propagation of event generated data applying the heartbeat common denominators at the core of both the military and First Responder/commercial Situational Awareness (SA) systems is key to realizing the goal of establishing an (inter) National Common Operational Picture. Symbolic interoperability and interoperable, temporally synchronized data exchange, adhoc spontaneous integration is the focus area of this series of method patent applications.

The heartbeat protocol and heartbeat XML schemas / messages as designed by the committees and organizations developing homeland defense / homeland security strategies will enable data sharing / workflows between the citizens of our homeland and first responders as consumers of situational awareness information gathered by our military(s) – provided that they arrive at agreement on the frequency that the heartbeat gathers network configuration data and places that data in queues, files structures, object stores and provided that the heartbeat network configuration XML messages apply common structures and application methodology.

This invention describes a method whereby network centric warfare (NCW) procedural methods currently applied to military networks in a proprietary method (e.g., Tactical Data Links or TADIL formats are military developed, unique binary formats as described in method patent application 10/605144 "method to commercialize structured military messaging") are commercialized then reapplied to commercial emergency networks (e.g., E9-1-1 Public Safety Answering Points – PSAPs).

This invention describes commercializing the methodology behind network centric warfare (NCW) whereby mission threads in military parlance (workflow logic / business rules) initiating message /data exchanges via unicast & multicast IP groups on the battlefield are similarly handled through the world's telecommunications Public Safety Answering Points – PSAPs so that soldiers will fight as they have trained in local neighborhoods if their supporting organic equipment is unavailable.

The base application 10/605144 describes a methodology where military unique FFIRNs (field item reference numbers and FUDNs (field unit number designators) that are three and four digit codes are converted to corresponding XML tags, those tags as part of XML form / messages will be processed by products like Microsoft Groove or Biztalk or any other product / enterprise suite with an intrinsic forms engine / XML parser. Application 10/605144 method to commercialize structured military messaging is a necessary precondition to executing the two continuation applications.

The first continuation method patent application 10/708000 "method to enable a Homeland Security Heartbeat" describes methodology enabling consistency of event timing / network configuration data harvesting across n complex systems for event data distribution and network (re) configuration and reconstitution based upon the TCP/IP heartbeat protocol that is a low level publish – subscribe mechanism in widespread use by both military and commercial systems – albeit applied differently (e.g., the heartbeat data sampling is set at different rates).

Application 10/708000 adds through the use of the heartbeat protocol's intrinsic timing function and data harvesting function adds temporal consistency and the ability to "spontaneously re-integrate" based on the military's research into organizational mobility via multicast / unicast router/switch groups stored in Management Information Bases – MIBS. .

Application 10/708000 describes a methodology whereas router-switch multicast groups for tactical-strategic military systems, first responder and commercial event-alert broadcast services are updated at heartbeat protocol set predefined intervals (e.g., milliseconds, seconds, & minutes). This multicast descriptive group data stored in Management Information Bases (MIBS) in router/switches is updated by data gathered by the heartbeat protocol as a type of publish subscribe mechanism. This network configuration data is then distributed by eXtensible Markup Language - XML heartbeat schema's / messages that are used to reconfigure unicast – multicast network parameters such as router – switch management information bases (MIBs).

This second continuation application 10/709358 is a continuation of 10/70800 that is a continuation of 10/605144. This invention describes a methodology whereby individuals or groups data subscriptions are updated via a common refresh rate for display on Emergency Action Center (EAC) screens and personal handheld wired and wireless devices (e.g., smart phones, personal digital assistants) applying a common symbology set as described by accessing common federal XML repositories described by common syntax e.g., Service Provisioning Markup Language (SPML) and Web Services Resource Framework (WSRF) that maintains state information essential in low bandwidth, mobile environments..

Referring to the 3rd Claim area 10/709358 Tool area in the diagram's main box describing Heartbeat e9-1-1 as a topology: Use of TCP/IP's heartbeat mechanisms as the basis for configuring network (router Management Information dataBase - MIB) is a key mechanism to exchange situational awareness information (where am I, where are my friends, where is the threat, what, when, how fast, how often) given that multicast group subscription methodology is currently implemented by the DOD and commercial sector alike.

3rd claim area 10/709358 Tool area includes the acronym UTO – Unit Task Order. The template military situational awareness applications FBCB2 and Blue Force Tracking) apply the Unit Task Order as hierarchical depiction of unit structure showing how units are organized for operations similar to corporate wiring diagrams. UTO distribution is enabled by the use of TCP/IP's heartbeat mechanisms described in 2nd claim area 10/708000 in terms of the heartbeat protocol's send to, get from and timer / data harvest trigger. Gathering network (re) configuration data used to update tactical / corporate organization / first responder's multicast subscription information based on unit / organizational mission posture change is key Heartbeat e9-1-1 methodology.

The commercial equivalent of the military proprietary UTO Tool composes heartbeat protocol gathered network (re) configuration data as a XML EDXL-DE formatted schema with military DDMS data as embedded islands or child schemas. Commercial equivalent UTO tools will exchange these network reconfiguration messages with military counterpart organizations. Tool functionality includes the feature to update corresponding MCG – MultiCast Group subscription data and Management Information Base (MIB). The UTO is part of the military TIMS (Tactical Internet Management System).

Describing the top most two blocks in the box in the 3rd claim area 10/709358 from left to right:

Top most left block labeled Workflow Logic / Unicast – Multicast subscription data: FBCB2 / Blue Force Tracking / Land Warrior as the military's main situational awareness propagation systems are workflow logic instantiated by scripts, defined by filters as implemented and broadcast by unicast / multicast IP groups supported by router/switches. Workflow is a commercial mainstay as is subscribing to filtered multicast group content. Since commercially supported first responders and corporate stakeholders networks are also supported by router/switch infrastructure, recognizing this fundamental commonality is one of the basis of claims of Heartbeat e9-1-1.

Top right block labeled XML repositories, NIEM, JXDM, DDMS, OpenGIS OGC, EDXL-DE formatted sets reference the: National Information Exchange Model - NIEM, Global Justice XML Data Model (Global JXDM), DoD Discovery Metadata Standard (DDMS), Open Geospatial Consortium – OGC. These repositories will provide XML tag repositories for the viewers / applications / browsers to formulate Common Alert Protocol – CAP schemas with Emergency Data Exchange Language Distribution Element

(EDXL-DE) formatted messages with child schemas and / or DDMS formatted data islands to bridge emergency response threads between .mil, .gov, .com, .org domains.

The Heartbeat K00.99 network configuration message initiates a sequence whereby other data dissemination messages are spawned stimulating operational, intelligence, logistics etc data cascades on the military side of the Heartbeat e9-1-1 equation. A commercial equivalent heartbeat message is needed to instantiate emergency message data cascades on the commercial, organizational side of the equation.

The Common Alert Protocol - CAP goal to provide "a standard method to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems" must be designed in a manner that is backwards compatible with current FBCB2 / Blue Force Tracking equipped units and forward compatible with Future Combat Systems equipped units that both employ the heartbeat protocol and heartbeat XML network configuration messages for forwards / backwards compatibility.

3rd claim area 10/709358 above the box and below the bracket labeled Service Oriented Architecture – SOA: DISA's Service Oriented Architecture (SOA) product (Amberpoint) employs an end to end heartbeat protocol, heartbeat XML message based system health monitor of the Network Centric Enterprise Service - NCES runtime environment that it is offering to all other agencies. Therefore, from foxhole to enterprise, the heartbeat protocol and heartbeat message schema exchange between DOD/military and commercial First Responder domains are key building blocks / common denominators to increase of the power of network centric warfare by enabling direct military – first responder collaboration mitigating the next (inter) national catastrophic event by improving response times, faster targeting refresh rates, common timing of event sampling and enabling consistent screen refresh rates displaying consistent symbol sets.

Expanding on the application of a Common Alert Protocol designed with child domain schemas / embedded with military DDMS tags, this invention application is asserting that the military notion of "stragglers" will suit commercial / Homeland Security domains by tracking organizations, units or high profile users. RFID tracked packages that stray from posted itineraries or routines are labeled as "stragglers". Stragglers on a Blue Force Tracking screen are shown as dimmed or grayed out icons as "stale" since they failed to report within established time limits.

Restructuring the Common Alert Protocol (CAP) by adding nested XML schema elements as data islands or derivative child domain CAP schemas are developed; the intent behind structured military messaging as driven by the TCP/IP heartbeat network reconfiguration process will be combined with a unified CAP structure or child structures to achieve a universal military / commercial, JIM (Joint Interagency, Multinational) domain "Heartbeat e9-1-1" service given North American Aerospace Defense Command – NORAD data is processed by the Public Safety Answering Points but not directly exchanged with the military fast movers (fighters) or air defense units. A recent Signal Magazine article quoted a 30 second web page refresh rate accordingly – too slow for targeting and tracking purposes.

Development of a methodology of nested CAP schema elements and / or derivative child schemas as shown to the right of the 3rd claim area in the included diagram enables the following described functionality:

Radio Frequency Identification RFID where RFID tags if the active type, send data to a network monitoring / relay that sends the date time stamp, service provider or organization data, GPS derived location etc as harvested by the TCP/IP primitive heartbeat mechanisms (2nd claim area) to a threat integration center via router/switches applying the principles behind Blue Force Tracking (BFT) (e.g., filtering applying business rules (mission thread logic in military speak) and FBCB2 as described in this patent and previous patent applications.

If a passive RFID tag, then the data and logic to process that data is contained is harvested by application of the TCP/IP send to, get from functions, as timed by the timing function that serves as a trigger to send the harvested data to the monitoring station for onward distribution heeding stored business logic (mission threads in military parlance) filtering methodology and procedures.

The application layer logic as carried out by scripts, methods or procedures performs the requisite association of the three and four digit codes that correspond to symbology derived from message data elements that correspond to geospatial symbols applied by geospatial applications such as ESRI's Joint Common Mapping Toolkit - JMTK.

The result of this methodology is that RFID tagged packages, devices or humans wearing RFID tagged bracelets will automatically generate situational awareness data that is granular to ten digit GPS location data and individual platforms and equipment vice general geometric areas of interest and non-GPS derived location data characteristic of the Common Alert Protocol current design.

3rd claim area 10/709358 bottom row description left to right:

This area is carried over from the first two method patent applications that used Groove Network's Groove (since acquired by Microsoft) software framework as an example of how a product inclusive of a forms engine (e.g., Microsoft InfoPath for Groove and Sharepoint) will import the converted proprietary military message sets as XML schemas for temporary storage in the XML Object Store until needed as monitored by the intrinsic state management engine prior to onward distribution or relay by the XML Object Relay that is descriptive of the Microsoft Groove product.

One of the Department of Homeland Security major projects is based upon Groove Technology and has been deployed to the local / city level thus setting the stage for Heartbeat e9-1-1. Microsoft Biztalk would be another option.

3rd claim area 10/709358 beneath the framework box description left to right:

Database / Joint Common Data Base: database technology for storage and non-real time replication / dissemination of XML tagged data timed by the heartbeat protocol.

Geospatial Information Systems (GIS): the prevalent category of enterprise infrastructure that would display / process heartbeat temporally timed event data drawn from common symbol – XML repositories. The GIS interacts with the object stores / object relay as managed by the state management engine of the Heartbeat e9-1-1 compliant solution.

The box labeled cellular, wireless, satellite with the radio Global Positioning System (GPS) label. Military tactical radios like commercial telecommunication cell / smart phones, laptops and handhelds include GPS chips for the geo location information that is part of what the heartbeat protocol harvests to determine unit / individual platform status (e.g., straggler, halt, moving, stale, or offline). This state data is harvested by sensor nets – military or commercial (e.g., the indicated Transducer Data Exchange Protocol TXDP & ZigBee 802.15.4 that both ride and make use of the heartbeat protocol).

The table below is a comparison of military unique awareness systems on the left with equivalent commercial, first responder, commercial stakeholder aspects on the right. This table serves as a reference to the methodology developed for the military systems inspiring network centric warfare such as Force XXI Battle Command Brigade and Below – FBCB2. FBCB2's satellite variations Blue Force Tracking and Joint Blue Forces Situational Awareness (JBFSA) that are code similar with timing parameters adjusted for satellite networks.

Land Warrior is a soldier worn adaptation of FBCB2 that is code similar. Together these systems that are generally speaking work flow logic executed data gathering and dissemination filter over multicast subscription technology typical of router-switch networks that have commercial counterpart systems in wide spread use today. Verizon VCAST is one such system that is well known.

Military // Homeland Defense .mil	Homeland Security, .com .org .gov
Well-known multicast groups	Subscription service providers for .com, .org, .net etc by domains maintaining customer / subscriber / employee multicast groups
Doctrinal multicast groups	Multicast groups by domain segment or by formal agreement (e.g., transportation, security, users by type, service, agency etc)
Moving unit, gaining unit of action, platform tethering, untethering to radio nodes / satellite on the move equipment	Platform or user / handoff subscriber node e.g., cell tower to tower. Satellite radio subscriber.
Command relationship (OPCON, attach), Unit of Action, Unit of Employment affiliations	Heartbeat 911 subscriber service, primary provider, affiliate provider, if roaming, affiliating, disaffiliating from cell towers
Effective Date/Time/Group (DTG) Block	Date / Time adjusted for Daylight Savings, world time zones
Synchronization Delta Time Block	Time when moving or traveling group executes network changes that change data distribution routes in supporting routers
UTR (U = Unit, T = Task, R = reorganization) command is broadcast to the entire net / subnet for execution	UTR = Unit Task Reorganization modified = Heartbeat XML network (re) configuration message sent containing data changing router Management Information Bases (MIBS) that change participation in multicast groups subscriptions reflecting organization structure. Enables military to join first responder nets and vice verse on an adhoc basis. Accounts for device mobility.
Affected platforms belonging to Moving Unit execute as per the Effective DTG.	Service providers router multi-cast groups change given organizational changes, user movements, pre-set time intervals
All others not affected execute at Synchronization Delta Time	Agreed upon time frame e.g., 5 seconds - 15 - 99 minutes for heartbeat protocol to harvest / refresh multicast subscriptions
The Heart Beat process incorporates the UTR command into the periodic Heartbeat message. This becomes the method by which "stragglers" or "stale" platforms re-affiliate / maintain network configuration synchronization	"Stragglers" i.e., Radio Frequency Identification Designation RFID tagged package(s), travelers, prisoners... not shipped / departed from a checkpoint or pattern is erratic. Deviation from schedule exceeding established parameters. Stale – no reports received for set periodic reporting period.
Task organization of the tactical internet Planning on when and what to change is critical to tactical maneuver / hasty reorg	Changing major network configurations based upon major events (Olympics), or anticipating major movements of subscribers (natural, manmade disasters), major corporate meeting

Table 1: Military unique awareness system attributes compared with commercial counterpart domains

ABSTRACT OF THE DISCLOSURE

Heartbeat e9-1-1 / Heartbeat e9-1-2* as a continuation of application entitled "Method to enable a Homeland Security Heartbeat as a continuation of the application entitled "Method to commercialize structured military messaging" involves reapplying Network Centric Warfare (NCW) methods commercially leveraging the world's network providers (Telco's) infrastructure that provide up to 80% of a military organization's leased network connectivity. Heartbeat e9-1-1 will improve interoperability & operational synergy via direct message/data exchanges reapplying war tested operational procedures that update router/switch multicast group subscriptions linking DOD Situational Awareness systems/networks to Telco Public Safety Answering Points – PSAPs applying regulations stipulating the use of the heartbeat

protocol and heartbeat eXtensible Markup Language (XML) schemas. Military situational awareness (SA) systems and telecommunication networks apply common denominators: the TCP/IP heartbeat protocol and heartbeat (XML) messages -- differently. When the DOD and the world's Telco networks agree on common network (re) configuration procedures based on these common denominators (heartbeat protocol and heartbeat eXtensible Markup Language (XML) EDXL-DE formatted schemas), direct data / message exchanges and collaboration based on common timing of events and common symbology will be possible.

* Note the "e9-1-2" designation is cited in the event the E9-1-1 Congressional Caucus selects e9-1-2 as the designation / numbering scheme that will incorporate method to enable Heartbeat e9-1-1 methods.

SEQUENCE LISTING

See diagram 1 and table 1 of this document. Different scenarios and different situations stimulate different work flow logic and filter logic activation as well as different message sets that are impractical to represent in a single document. Military systems of systems testing comprise hundreds if not thousands of mission threads (analogous to commercial business logic) shown in state, flow and sequence diagrams. Different scenarios flow differently through the enterprise architectures which are different. A generic topology was used vice architecture to represent a generic, universally applicable methodology that will be implementable across n complex systems in an application, product, and operating system neutral method.